CLAIMS

What is claimed is:

1. A method for providing hardware support for memory protection and virtual memory address translation for a virtual machine, comprising:

executing a host machine application within a host machine context;

executing a virtual machine application within a virtual machine context;

storing a plurality of TLB (translation look aside buffer) entries for the virtual machine context and the host machine context within a TLB; and

logically combining memory protection bits for the plurality of TLB entries to enforce memory protection on the virtual machine application.

2. The method of claim 1 wherein at least one of the memory protection bits is a dirty bit.

3. The method of claim 1 wherein at least one of the memory protection bits is a read/write bit.

4. The method of claim 1 wherein the memory to protection bits are combined using a logical and operation.

5. The method of claim 1 wherein the host machine application is a host machine operating system that executes within the host machine context and the virtual machine application is a virtual machine operating system that executes within the virtual machine context.

6. The method of claim 1 wherein the TLB entries include respective context identifiers enabling the TLB entries to provide physical address translation for virtual addresses from both the host machine context and the virtual machine context.

7. The method of claim 1 further comprising:

updating the TLB with new entries when a virtual machine TLB miss occurs or a host machine TLB miss occurs.

8. A system for providing hardware support for memory protection and virtual memory address translation for a virtual machine, comprising:

a processor architecture including micro architecture code configured to execute natively on a CPU hardware unit of the processor architecture; and

an address translation cache for implementing a translation look aside buffer, with the address translation cache in conjunction with the processor architecture implementing a method comprising:

executing a host machine application within a host machine context;

executing a virtual machine application within a virtual machine context;

storing a plurality of TLB (translation look aside buffer) entries for the virtual machine context and the host machine context within a TLB; and

logically combining memory protection bits for the plurality of TLB entries to enforce memory protection on the virtual machine application.

9. The system of claim 8 wherein at least one of the memory protection bits is a dirty bit.

10. The system of claim 8 wherein at least one of the memory protection bits is a read/write bit.

11. The system of claim 8 wherein the memory to protection bits are combined using a logical and operation.

12. The system of claim 8 wherein the host machine application is a host machine operating system that executes within the host machine context and the virtual machine application is a virtual machine operating system that executes within the virtual machine context.

13. The system of claim 8 wherein the TLB entries include respective context identifiers enabling the TLB entries to provide physical address translation for virtual addresses from both the host machine context and the virtual machine context.

14. The system of claim 8 further comprising:

updating the TLB with new entries when a virtual machine TLB miss occurs or a host machine TLB miss occurs.

15. A computer readable media for providing hardware support for memory protection and virtual memory address translation for a virtual machine, the media storing computer readable code which when executed by a processor causes the processor to implement a method comprising:

executing a host machine application within a host machine context;

executing a virtual machine application within a virtual machine context;

storing a plurality of TLB (translation look aside buffer) entries for the virtual machine context and the host machine context within a TLB; and

logically combining memory protection bits for the plurality of TLB entries to enforce memory protection on the virtual machine application.

16. The computer readable media of claim 15 wherein at least one of the memory protection bits is a dirty bit.

17. The computer readable media of claim 15 wherein at least one of the memory protection bits is a read/write bit.

18. The computer readable media of claim 15 wherein the memory to protection bits are combined using a logical and operation.

19. The computer readable media of claim 15 wherein the host machine application is a host machine operating system that executes within the host machine context and the virtual machine application is a virtual machine operating system that executes within the virtual machine context.

20. The computer readable media of claim 15 wherein the TLB entries include respective context identifiers enabling the TLB entries to provide physical address translation for virtual addresses from both the host machine context and the virtual machine context.

21. The computer readable media of claim 15 further comprising:

updating the TLB with new entries when a virtual machine TLB miss occurs or a host machine TLB miss occurs.